ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28004-4— 2018

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 4

Дополнительное специальное руководство по внедрению ИСО 28000, когда соответствие ИСО 28001 является целью менеджмента

(ISO 28004-4:2014, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective, IDT)

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации оборонной продукции и технологий» (ФГУП «Рособоронстандарт») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен ФГУП «Стандартинформ»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 июля 2018 г. № 436-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28004-4:2014 «Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ИСО 28000. Часть 4. Дополнительное специальное руководство по внедрению ИСО 28000, когда соответствие ИСО 28001 является предметом менеджмента» (ISO 28004-4:2014 «Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective», IDT).

Международный стандарт разработан Техническим комитетом ISO/TC 8 «Суда и морские технологии».

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут являться объектами патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Настоящий стандарт подготовлен с целью дополнения основных положений ИСО 28004-1 в части использования наилучших практик, приведенных в ИСО 28001 в качестве цели менеджмента в международных цепях поставок.

Дополнительное руководство, изложенное в настоящем стандарте, не противоречит общему руководству, изложенному в ИСО 28004-1.

ИСО 28004-1 представляет собой общее руководство, содержащее основные положения и рекомендации по внедрению ИСО 28000, которые способствуют лучшему пониманию его требований.

ИСО 28001 и ИСО 28000 не противоречат друг другу несмотря на более конкретизированные технические требования безопасности, изложенные в ИСО 28001.

Применение настоящего стандарта помогает соответствовать критериям безопасности уполномоченного экономического оператора.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 4

Дополнительное специальное руководство по внедрению ИСО 28000, когда соответствие ИСО 28001 является целью менеджмента

Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 4. Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective

Дата введения — 2019—06—01

1 Область применения

Настоящий стандарт содержит дополнительное руководство для организаций, внедряющих ИСО 28000 и желающих использовать приведенные в ИСО 28001 наилучшие практики в качестве цели менеджмента в международных цепях поставок. Наилучшие практики, изложенные в ИСО 28001, помогают организациям определять и документировать уровни безопасности внутри международной цепи поставок, а также способствуют процессу валидации в национальных программах уполномоченного экономического оператора (далее — УЭО), которые разработаны в соответствии с рамочными стандартами безопасности Всемирной таможенной организации (далее — ВТО).

Настоящий стандарт не является самостоятельным документом. Основная часть ИСО 28004-1 предусматривает руководство, относящееся к необходимым входным данным, процессам, выходным данным и другим требуемым ИСО 28000 элементам. В настоящем стандарте изложено дополнительное специальное руководство по внедрению ИСО 28000, когда соответствие ИСО 28001 является целью менеджмента.

Некоторые требования, установленные в программе УЭО ВТО, относятся к функциям органов исполнительной власти и не рассматриваются в международных стандартах ИСО. Они включают:

- демонстрируемое соответствие таможенным требованиям. Таможенные органы при рассмотрении запроса о статусе УЭО должны принимать во внимание демонстрируемое соответствие событий, предшествующих получению статуса;
- соответствующую требованиям систему управления коммерческими записями. Статус УЭО обязывает поддерживать своевременные, точные, полные и верифицируемые записи, связанные с импортом и экспортом. Поддержание верифицируемых коммерческих записей является необходимым элементом безопасности международной торговой цепи поставок;
- финансовую устойчивость. Финансовая устойчивость УЭО является важным индикатором способности поддерживать и улучшать меры обеспечения безопасности цепи поставок;
- консультации, сотрудничество и обмен информацией. Таможенные, другие компетентные органы и УЭО на всех уровнях — международном, национальном и местном — должны регулярно оказывать консультации по вопросам, представляющим взаимный интерес, включая безопасность цепи поставок и меры снижения ограничений, таким образом, чтобы не ставить под угрозу осуществление их деятельности. Результаты таких консультаций должны способствовать развитию и поддержанию имеющейся в таможенных органах стратегии менеджмента риска.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные нормативные документы. Для датированных ссылок применяют только указанное издание ссылочного документа. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения):

Издание официальное

ISO 20858, Ships and marine technology — Maritime port facility security assessments and security plan development (Суда и морские технологии. Оценки безопасности морских портовых сооружений и разработка плана обеспечения безопасности)

ISO 28000, Specification for security management systems for the supply chain (Системы менеджмента безопасности цепи поставок. Технические условия)

ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности в цепи поставок, оценки и планы. Требования и руководящие указания)

ISO 28004-1, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles (Системы менеджмента безопасности цепи поставок. Руководство по внедрению ИСО 28000. Часть 1. Основные принципы)

3 Общие сведения

Рисунок 1 иллюстрирует, как соответствие и возможная сертификация по ИСО 28000, включающему наилучшие практики, приведенные в ИСО 28001, дополняют требования национальных, региональных программ или программ УЭО, а также определенные промышленные программы, содействуя их валидации.

Организации также могут выбрать соответствие ИСО 28000 и ИСО 28001 для улучшения и документирования менеджмента безопасности цепи поставок без цели получения сертификации УЭО.

Рисунок 1 — Стандарты безопасности, дополняющие друг друга в части обеспечения безопасности цепи поставок

4 Структура настоящего стандарта

В разделе 5 приведены таблицы, в которых отражены объединенные требования рамочных стандартов безопасности ВТО к УЭО, а также разделы ИСО 28000 и ИСО 28001, в которых представлены требования к УЭО.

Раздел 6 содержит практическое руководство для включения различных требований ИСО 28001 в ИСО 28000 в качестве входных данных, процессов или выходных данных.

Раздел 7 содержит замечания для разъяснения незначительных различий в терминологии, используемой в ИСО 28000 и ИСО 28001.

5 Объединенные требования рамочных стандартов безопасности Всемирной таможенной организации к уполномоченному экономическому оператору

В таблицах 1—9, приведенных в настоящем разделе, требования к УЭО выделены жирным шрифтом. Далее следует краткое изложение этого требования. Ниже, в следующей строке, указаны разделы ИСО 28000 и ИСО 28001, в которых рассмотрены эти требования. Большинство требований к УЭО ВТО приведены в таблицах 1—9, включая требования, которые определены как функции государственных органов во введении. Следует отметить, что национальные программы УЭО могут иметь дополнительные требования, в том числе специальные минимальные критерии, которые могут быть рассмотрены в ИСО 28000 или ИСО 28001 не в полном объеме.

Таблица 1

A. Обучение, подготовка и осведомленность
Таможенные органы и операторы УЭО должны разработать механизмы для обучения и подготовки персонала относительно политики безопасности, распознавания отклонений от этой политики и понимания действий, которые должны быть предприняты в ответ на ошибки в обеспечении безопасности
ИСО 28000, 4.4.2 (Компетентность, подготовка и осведомленность) ИСО 28001, 5.3.1 (Персонал, проводящий оценку)

Таблица 2

B. Обмен информацией, доступность и конфиденциальность
Таможенные органы и операторы УЭО, являясь частью общей комплексной стратегии защиты конфиденциальной информации, должны разработать или улучшить способы защиты охраняемой информации от неправильного использования или несанкционированного изменения
ИСО 28000, 4.2 (Политика в области безопасности), 4.4.5 (Управление документами и данными), 4.5.4 (Управление записями) ИСО 28001, 5.8 (Защита информации по обеспечению безопасности и охраны)

Таблица 3

C. Безопасность груза
Таможенные органы и операторы УЭО должны определить и/или проводить комплекс мероприятий, гарантирующих целостность грузов и самый высокий возможный уровень средств контроля доступа, а также установить стандартные процедуры, способствующие безопасности груза
ИСО 28000, 4.4.6 (Управление операциями) ИСО 28001, 5.4 (Разработка плана обеспечения безопасности цепи поставок)

Таблица 4

D. Безопасность транспортных средств
Таможенные органы и операторы УЭО должны проводить совместную работу, направленную на установление эффективных режимов контроля при отсутствии национальных или международных документов по обеспечению эффективной защиты и надлежащего обслуживания транспортных средств
ИСО 28000, 4.4.6 (Управление операциями) ИСО 28001, 5.4 (Разработка плана обеспечения безопасности цепи поставок)

Таблица 5

E. Безопасность помещений
Таможенные органы после принятия во внимание положений статуса УЭО и необходимого соответствия обязательным международным стандартам должны установить требования по внедрению особых таможенных протоколов повышения безопасности, которые обеспечивают безопасность зданий, а также мониторинг и контроль внешнего и внутреннего периметров
ИСО 28000, 4.4.6 (Управление операциями) ИСО 28001, 5.4 (Разработка плана обеспечения безопасности цепи поставок)

Таблица 6

F. Безопасность персонала
Таможенные органы и операторы УЭО должны на основе своих полномочий и компетенций защищать персональные данные предполагаемых работников в рамках закона. Кроме того, они должны запрещать несанкционированный доступ к сооружениям, транспортным средствам, погрузочным платформам и грузовым площадкам, который может повлиять на безопасность этих объектов на участках цепи поставок, находящихся под их ответственностью
ИСО 28000, 4.4.6 (Управление операциями) ИСО 28001, 5.4 (Разработка плана обеспечения безопасности цепи поставок)

Таблица 7

G. Безопасность торговых партнеров
Таможенные органы должны установить требования к УЭО и механизмы, при помощи которых может быть поддержана безопасность глобальной цепи поставок через заинтересованность торговых партнеров в добровольном повышении своих мер безопасности
ИСО 28000, 4.4.6 (Управление операциями) ИСО 28001, 4.1 (Паспорт участка цепи поставок), 4.2 (Деловые партнеры), 4.3 (Свидетельства о соответствии, принятые в международной практике), 4.4 (Деловые партнеры, освобождаемые от предъявления Декларации об охране), 4.5 (Область применения)

Таблица 8

H. Кризис-менеджмент и восстановление в случае инцидента
Для того чтобы минимизировать последствия катастроф или террористических действий, кризис-менеджмент и процедуры по восстановлению должны включать перспективное планирование и установление процессов управления в подобных чрезвычайных обстоятельствах
ИСО 28000, 4.5.3 (Сбои, инциденты, несоответствия в отношении безопасности, корректирующие и предупреждающие действия), 4.4.6 (Управление операциями), 4.4.7 (Готовность к действиям в чрезвычайной ситуации, реагирование и восстановление безопасности) ИСО 28001, 5.7 (Меры, принимаемые после реализации инцидентов в области обеспечения безопасности)

Таблица 9

I. Оценка, анализ и улучшение
Операторы УЭО и таможенные органы должны планировать и внедрять процессы мониторинга, оценки, анализа и улучшения, чтобы: - оценить согласованность с настоящими руководящими указаниями; - обеспечить целостность и адекватность системы менеджмента безопасности; - определить потенциальные сферы улучшения системы менеджмента безопасности с целью повышения безопасности цепи поставок
ИСО 28000, 4.1 (Общие требования), 4.3 (Оценка рисков в области безопасности и планирование) ИСО 28001, 5.1 (Процесс обеспечения безопасности и охраны цепи поставок. Общие положения) 5.2 (Идентификация масштабов оценки в области безопасности), 5.3.2 (Процесс оценки), 5.4 (Разработка плана обеспечения безопасности цепи поставок), 5.5 (Реализация плана обеспечения безопасности цепи поставок), 5.6 (Документирование и мониторинг процессов обеспечения безопасности и охраны цепи поставок)

6 Практическое руководство по включению требований ИСО 28001 в качестве входных данных, процессов или выходных данных при применении ИСО 28000

ИСО 28000	**Включение наилучших практик, приведенных в** ИСО 28001	**Комментарии**
4.2 Политика в области безопасности	Положение политики, которое устанавливает, где будут применены наилучшие практики. Эта информация может быть получена из документации по информации, требуемой в ИСО 28001 (4.1 a и b)	Организации, которые используют наилучшие практики с конечной целью утверждения статуса УЭО, должны проводить переговоры с таможенными органами, имеющими полномочия присваивать статус УЭО, чтобы гарантировать соответствие намеченной области применения наилучших практик требованиям для получения статуса УЭО
4.3.1 Оценка рисков в области безопасности	Пункт 5.3.1 определяет навыки и знания персонала, который будет проводить оценку в области безопасности. Пункт 5.3.2 устанавливает требование в части включения сценариев угроз, необходимых, по мнению уполномоченных должностных лиц, в добавление к сценариям, предложенным персоналом, проводящим оценку. Требуемая документация: a) все рассмотренные сценарии угроз безопасности; b) процессы, используемые при оценке этих угроз; c) все установленные и приоритетные контрмеры	ИСО 28001 не требует от организаций в цепи поставок, которые имеют международные сертификаты или одобрения (как определено в 4.3) или которые были сертифицированы на соответствие стандарту менеджмента, включающему или ИСО 20858, или ИСО 28001, повторно проводить оценки в области безопасности участков цепи поставок, ранее прошедших оценку (см. 4.4). Примечание — Если требуется подтверждение или сертификация статуса УЭО, то соответствующий таможенный орган или орган по сертификации, включенный в процесс, должен определить выбор международных сертификатов или одобрений и сертификации. В 4.2 ИСО 28001 указано, что некоторые деловые партнеры по цепи поставок могут не выразить желания участвовать в оценке в области безопасности для каждой вовлеченной компании. В таких случаях ИСО 28001 позволяет этим компаниям представить в письменной форме меры по безопасности, которые они будут обеспечивать (декларации об охране). Достоверность этих деклараций должна быть проверена согласно 4.5
4.3.1 Разработка плана обеспечения безопасности	Подраздел 5.4 определяет требования разработанного плана обеспечения безопасности для охватываемых участков цепи(ей) поставок. Организациям при разработке и пересмотре своих планов обеспечения безопасности необходимо рассмотреть для использования руководство, представленное в приложениях A и B	
		В ИСО 28001 (начиная с 5.5 и заканчивая 5.6.2) установлены следующие требования: разработанный план обеспечения безопасности должен быть внедрен и контролироваться в качестве части системы менеджмента
4.5.3 Сбои, инциденты, несоответствия в отношении безопасности, корректирующие и предупреждающие действия	В подразделе 5.7 дополнительно установлено требование относительно того, что в случае нарушения безопасности организация следовала процедурам отчетности перед таможенными и/или соответствующими правоохранительными органами	

7 Замечания по терминологии

Существуют некоторые различия в терминологии ИСО 28000 и ИСО 28001. Поэтому необходима более подробная информация, касающаяся связи конкретных терминов, используемых в указанных стандартах. Данный раздел приводит более подробную информацию, отвечающую этой необходимости.

Термины по ИСО 28000 **и** ИСО 28004	**Термины по** ИСО 28001	**Комментарии**
Средство, подраздел 3.1	Активы, подраздел 3.2	Значения и определения этих двух терминов синонимичны в ИСО 28000 и ИСО 28001
Программы в области менеджмента безопасности, подраздел 3.6		Это элемент системы менеджмента. Программа обеспечения безопасности, приведенная в ИСО 28001, может быть рассмотрена как подобная программа
Причастная сторона, подраздел 3.8	Деловой партнер, подраздел 3.4	Причастная сторона определена в ИСО 28000 и включает большое количество организаций с законными интересами в работе системы менеджмента безопасности. Деловой партнер определен в ИСО 28001 как организация — участник цепи поставок с имеющимися деловыми связями. Деловые партнеры могут считаться подгруппой более широкой группы причастной стороны
	Организация — участник цепи поставок, подраздел 3.15	Причастная сторона определена в ИСО 28000 как организация — участник цепи поставок, которая производит, оперирует, транспортирует или обрабатывает грузы или соответствующую информацию цепи поставок согласно ИСО 28001
	Международные цепи поставок, подраздел 3.12	ИСО 28001 определяет этот термин как цепь поставок, которая в некоторых точках пересекается с международной или экономической границей. Поскольку не все цепи поставок пересекаются с границами, международная цепь поставок может считаться сокращенным вариантом определения цепи поставок, данного в ИСО 28000
Риск, подраздел 3.10	Учет инцидентов в области обеспечения безопасности, (подраздел В.5, шаг 4)	Хотя термин «риск» не определен в ИСО 28001, он четко сформулирован как сочетание вероятности и последствий в нескольких частях ИСО 28001, в которых рассмотрены учет инцидентов в области обеспечения безопасности и разработка контрмер
Угроза, подраздел 3.3	Сценарий угрозы, подраздел 3.27. Инцидент в области обеспечения безопасности, подраздел 3.21. Последствие, подраздел 3.6. Цель, подраздел 3.26	ИСО 28000 определяет термин «угроза» как возможное действие или серию действий, способных наносить ущерб для любой из причастных сторон. Слово «преступный» может подразумеваться перед словом «действие», так как система менеджмента зависит от безопасности. ИСО 28001 разбивает термин «угрозы» на четыре части (подразделы 3.27, 3.21, 3.26 и 3.6), которые совместно определяют сценарий потенциальной угрозы, и цель, которая может приводить к инциденту с последствиями
	Область деятельности, подраздел 3.17 (это элемент декларации о применении — 4.1)	ИСО 28001 определяет этот термин как функции, которые осуществляет организация — участник цепи поставок, а также где именно она их осуществляет. Эта концепция содержится в обсуждении в ИСО 28004-1, которое имеет отношение к определению границ и области применения системы менеджмента

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 20858	—	*
ISO 28000	—	*
ISO 28001	—	*
ISO 28004-1	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

УДК 656.614.3.004:006.354 ОКС 03.100.01

Ключевые слова: менеджмент безопасности, цепь поставок, угрозы, менеджмент риска

БЗ 6—2018/73

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 30.07.2018. Подписано в печать 08.08.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,24.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru